Desarrollo Seguro en Python

Lección 3: OWASP TOP 10 Controles Proactivos

eip ESCUELA INTERNACIONAL POSGRADOS

Aplicando controles proactivos

Trabajas como responsable de ciberseguridad en una empresa de desarrollo software para SALUD. El acceso a la aplicación se hace con factor de doble autenticación (certificado digital + envío clave móvil). Una vez dentro una de las opciones es añadir información a la Historia Clínica del paciente mediante un formulario de recogida de datos que tiene los siguientes campos: fecha, anamnesis, datos de exploración, diagnóstico, pronóstico y tratamiento. Los datos personales los carga automáticamente ya que los pacientes están dados de alta en el sistema. Como tal estamos ante una entrada de datos al sistema. Utilizando la guía de controles proactivos y la guía de Seguridad de las TIC CCN-STIC 857 (Requisitos de seguridad para Aplicaciones de Cibersalud en el contexto del Esquema Nacional de Seguridad) indica todo lo necesario relativo a seguridad de desarrollo software que habría que hacer con esos datos desde que se recogen hasta que se almacenan en la base de datos.

Objetivos

- Aplicar controles proactivos.
- Aplicar recomendaciones de la guía de Seguridad de las TIC CCN-STIC 857

Contenido correspondiente a lección 3: OWASP TOP 10 CONTROLES PROACTIVOS

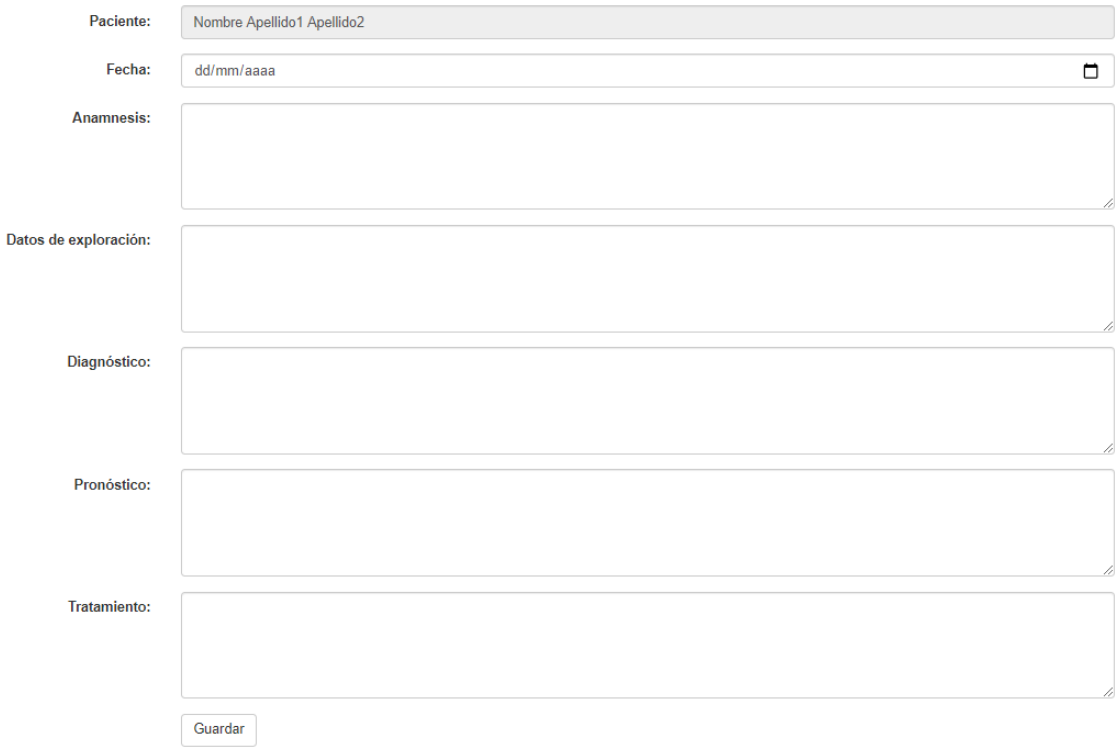
Actividad relacionada con la lección 3:

A continuación se describe el formulario y los tipos de datos que se especifican en los requisitos.

Paciente: datos que se recuperan de la base de datos y no se pueden modificar.

Fecha: campo de tipo fecha (día/mes/año)

Campos de tipo texto: anamnesis, datos de exploración, diagnóstico, pronóstico y tratamiento.



Estos campos se guardan en una tabla de la base de datos relacional que se llama **HistoriaClinica** y esta vinculada con la tabla **Pacientes** donde esta la información personal de todos los pacientes.